

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

JACOB RAINES,
[DOB: 3/31/1979],

Defendant.

Case No. 16-00064-01-CR-W-HFS

COUNT ONE:

**Access with Intent to View Child Pornography
Over the Internet**

18 U.S.C. §§ 2252(a)(4) & (b)(2)

NMT: 10 Years Imprisonment

NMT: \$250,000 Fine

Supervised Release: 5 Years to Life

Class C Felony

COUNT TWO:

Computer Intrusion/Fraud

18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i)

& (c)(2)(B)(iii)

NMT: 5 Years Imprisonment

NMT: \$250,000 Fine

Supervised Release: NMT 3 Years

\$100 Mandatory Special Assessment

Each Count

Forfeiture Allegation

S U P E R S E D I N G I N F O R M A T I O N

THE UNITED STATES ATTORNEY CHARGES THAT:

COUNT ONE

Between on or about November 13, 2013, and March 28, 2014, in the Western District of Missouri and elsewhere, **JACOB RAINES**, defendant herein, knowingly accessed one or more films, videotapes, and other matter which contained visual depictions, that had been shipped and transported in interstate and foreign commerce by any means including by computer, and which were produced using materials which had been shipped and transported in or affecting interstate or foreign commerce by any means including by computer; and the production of the visual

depictions involved the use of minors engaging in sexually explicit conduct, and were visual depictions of such conduct, in violation of Title 18, United States Code, Sections 2252 (a)(4) and (b)(2).

BACKGROUND FOR COUNT TWO

1. Beginning on or about July 6, 2004, and continuing through on or about March 28, 2014, the defendant, Jacob Raines, worked as the IT Manager for a company in Kansas City, Kansas.

2. Approximately two weeks after the defendant resigned from this company, another individual filled the IT Manager role at the company. The new IT Manager removed the defendant's computer passwords and made other security changes consistent with the transition to a new IT Manager.

3. On or about May 19, 2014, the new IT Manager utilized the computer that had previously been assigned to the defendant, and discovered the computer had accessed the company's unique and proprietary source code files and the computer had an open File Transfer Protocol connection, which allowed the defendant to remotely access the company's source code files and copy them to an off-site server in Parkville, Missouri.

4. The defendant had utilized a Remote Desktop Protocol to access the company's server, and the logs revealed the defendant had accessed and copied the proprietary source code with the File Transfer Protocol to another server, at least on May 16-18, 2014.

COUNT TWO

5. Paragraphs one through four are incorporated as though fully set out herein.

6. From on or about May 16, 2014, and continuing through on or about May 19,

2014, in the Western District of Missouri and elsewhere, the defendant, **JACOB RAINES**, intentionally accessed a computer belonging to a company in Kansas City, Kansas, without authorization, and obtained information from that protected computer, which was sent to the defendant's private server in Missouri. This offense was committed for the purpose of commercial advantage and private financial gain, and the value of the information obtained exceeded \$5,000.

7. This was in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

FORFEITURE ALLEGATION

The allegations contained in Count One are realleged and are incorporated by reference herein for the purpose of alleging forfeiture of: any visual depiction described in Title 18, United States Code, Section 2252, or any film, videotape, or other matter which contains any such visual depiction, which was transported, mailed, shipped, or received in violation of these sections; any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offenses; and any property, real or personal, used or intended to be used to commit or to promote the commission of such offenses; including, but not limited to the following:

1. A Memorex DVD with a handwritten "X" over the x in Memorex, labeled "Room K, Log No. 12";
2. A Western Digital WD3200AAKS 320 Gigabyte SATA hard drive, serial number WMAV2U331404;
3. A Dell Optiplex 980 Desktop computer with service tag 9R59RL1;

- All in violation of Title 18, United States Code, Section 2253.

Thomas M. Larson
Acting United States Attorney

Dated: May 23, 2017